

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

MAY 14 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

IN THE MATTER OF THE SEARCH OF INFORMATION
THAT IS STORED AT PREMISES CONTROLLED BY
GOOGLE LLC, 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA 94043

Case No. 4:19 MJ 7175 SPM

APPLICATION FOR A SEARCH WARRANT

I, Special Agent Christopher Faber, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A - PROPERTY TO BE SEARCHED

located in the SOUTHERN District of CALIFORNIA, there is now concealed

SEE ATTACHMENT B - ITEMS TO BE SEIZED AND SEARCHED

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18:1951
18:924(c)


Offense Description

Interfering with commerce by threats of violence
Possession of a firearm in furtherance of a crime of violence

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE


- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Christopher Faber, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: May 14 2019City and state: St. Louis, MO
Judge's signature

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Thomas J. Mehan

FILED

MAY 14 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST LOUIS

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED
INDIAA764@GMAIL.COM, and
AINEYOLA.CA@GMAIL.COM THAT
ARE STORED AT PREMISES
CONTROLLED BY GOOGLE, LLC.

Case No. 4:19 MJ 7175 SPM

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Christopher Faber, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with [a] certain account[s] that is stored at premises controlled by GOOGLE, LLC, an e-mail provider headquartered at 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require GOOGLE, LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation, and have been so employed since **July 2009**. As such, I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7), that is, an

officer of the United States empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516(1).

3. I am currently assigned to the St. Louis Division of the Federal Bureau of Investigation's Violent Crime Task Force, where I investigate violent crimes, to include robberies, carjackings, and fugitives. I am familiar with and have used normal methods of investigation, including, but not limited to, visual surveillance, questioning of witnesses, search and arrest warrants, informants, pen registers, precision location information, confidential sources and undercover agents, and court-authorized wire interceptions.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1951 and 924(c)(1), as more fully described in Attachment A, have been committed by JUSTIN MCGEE and CURTIS ALLEN. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).]

PROBABLE CAUSE

6. Since October 2018, the St. Louis Metropolitan Police Department and the FBI have been investigating a series of armed commercial robberies occurring at various locations

within the Saint Louis region, Eastern District of Missouri. All of the targeted facilities are in or affect interstate commerce. All of the events, some of which are detailed below, are believed to have been perpetrated by the same individual. It is believed the series of robberies were committed by JUSTIN MCGEE (black/male, DOB 06/11/81, alias name of “P”, “P-Dog”, “PD”, or some variation thereof). This belief is based on surveillance images, modus operandi, laboratory analysis, and other factors.

7. In each of the events, the Suspect is described by witnesses as, and/or can be seen on video surveillance footage as, a black male, approximately 25 to 40 years of age, approximately 5’07” to 6’00” tall, with a medium build, and “goatee” style facial hair. In each of the robberies, the Suspect has been observed wearing dark framed sunglasses. Unique clothing has also been described by witnesses and captured on surveillance video. For example, in two of the robberies, the Suspect is observed wearing a green ball cap and long sleeve, camouflage shirt with the gold lettering “Lennox Brigade” displayed on the front. Additionally, in most of the robberies, the Suspect has been observed utilizing either a semi-automatic handgun with a stainless steel slide and a black frame or an all-black semi-automatic handgun that is held in his right hand.

8. **Gamestop:** On or about October 17, 2018 at approximately 4:00 pm, a robbery occurred at the Gamestop located at 3702 S. Kingshighway, St. Louis, Missouri, which is documented per Saint Louis Metropolitan Police Department complaint number 18-049447. A single Suspect entered the business and walked to the counter. The Suspect spoke with two store employees and inquired about various merchandise. The Suspect then brandished a black handgun and pushed one employee to the ground while yelling “Open the register.” The second employee complied and then was commanded to open a second register by the Suspect. The

Suspect reached into the registers to remove the cash. The Suspect asked the employee to open the safe, but was told that only a manager could do so. The Suspect then fled the scene with approximately \$796 United States currency. The Suspect was described as wearing sunglasses and a long sleeve camouflage shirt with the words "Lennox Brigade". An area canvas conducted after the robbery yielded the described camouflage shirt and sunglasses, discarded near the location of the robbery. Subsequent laboratory examination of the clothing conducted by the St. Louis Metropolitan Crime Laboratory resulted in a CODIS hit that came back to JUSTIN MCGEE.

9. **T-Mobile:** On or about October 12, 2018 at approximately 7:50 pm, a robbery occurred at the T-Mobile located at 238 N. Highway 67, Florissant, Missouri, which is documented per Florissant Police Department complaint number 18-007131. A single Suspect entered the business and approached a store employee to inquire about recharging a phone. The Suspect then brandished a black handgun in his right hand, and said "Bitch, I'll fucking kill you." The Suspect ordered the employee to a rear office, where a manager was working. The Suspect ordered the manager to open three registers, and the Suspect removed cash from all three registers. The Suspect ordered both employees to the ground and ordered them to count to thirty while he fled the scene with approximately \$1300 United States currency. A review of video surveillance revealed the Suspect was wearing a camouflage shirt with gold lettering, similar in appearance to the shirt discarded in the aforementioned Gamestop robbery.

10. **Boost Mobile:** On, or about, February 4, 2019, at approximately 4:00 pm, a robbery occurred at the Boost Mobile, 79 North Oaks Plaza, Northwoods, Missouri, which is documented per Northwoods Police Department complaint number 19-0050. A single Suspect entered the business while talking on a cellphone. The Suspect approached a store employee and

stated he wanted to pay his phone bill. The Suspect then brandished a handgun and began to walk behind the counter. The employee retrieved his personal handgun and fired several rounds at the Suspect, possibly striking the Suspect. The Suspect then fled the scene. It was later determined through a CODIS hit of a DNA profile derived from blood evidence left at the scene, that JUSTIN MCGEE was suspected of committing the robbery.

11. **Smoothie King:** On, or about, November 23, 2018, at approximately 8:55 pm, a robbery occurred at the Smoothie King, 4475 Forest Park Avenue, St. Louis, Missouri, which is documented per Saint Louis Metropolitan Police Department complaint number 18-055640. The Suspect entered the store, approached the register, and reached for his right side as if he was reaching for a handgun. The Suspect told store employees: "I don't want any problems, just open the register." The employees complied, and the Suspect ordered them to the ground. The Suspect then took approximately \$240 United States currency from the register and left the building.

12. The subsequent investigation produced video surveillance of the Suspect exiting Smoothie King after the robbery. The Suspect apparently placed a phone call as he walked away from Smoothie King. Meanwhile, other video evidence produced images of a dark colored Chevrolet Impala which was parked nearby. As the robbery Suspect made the phone call, the driver of the Impala appeared to receive a phone call on his cellular phone. At this time, the Chevrolet Impala left a parked location and followed the path of the suspect, who walked from the scene of the robbery. Eventually, the Chevrolet Impala stops partially off camera view; where it is believed the Impala picked up the robbery Suspect off camera. It should be noted, this surveillance video produced images of the suspect vehicle's Missouri license plate FP0J9H.

13. **Family Dollar:** On, or about, December 25, 2018, at approximately 4:30 pm, a robbery occurred at the Family Dollar, 3501 North Kingshighway Boulevard, St. Louis, Missouri, which is documented per Saint Louis Metropolitan Police Department complaint number 18-060734. The Suspect entered the store holding his hand over his face, and asked a store manager about pain medication. After retrieving a box of pain medication, the Suspect walked to the register and brandished a black framed semi-automatic handgun with a stainless slide, which had been concealed beneath his coat, and ordered the store employees to the ground. The Suspect demanded an employee open the register, and the employee complied. The Suspect left the scene with approximately \$941.53 in United States currency and a 3SI Tracking Device which had been concealed within a bundle of currency.

14. The subsequent investigation produced 3SI GPS Tracking information. By coordinating GPS tracking information with video surveillance, investigators believe the suspect made his escape in the same Chevrolet Impala utilized during the Smoothie King robbery which occurred on, or about, November 23, 2018.

15. Still images from both business robberies compiled by the Saint Louis Metropolitan Police Department's Crime Analysis Unit revealed the vehicles used in both incidents is the same Chevrolet Impala. It should be noted, Investigators later met with the owner of this Chevrolet Impala, identified as India Finger. Finger viewed the surveillance photographs of vehicle used in the aforementioned robberies which had been compiled by the Crime Analysis Unit and positively identified the vehicle used in the robberies as belonging to her. Finger was provided with the dates of both robberies and advised she was at work both days. Finger further stated the father of her child, identified as CURTIS ALLEN (black/male,

DOB 08/19/77), had her vehicle on these dates. Finger stated no-one besides her and ALLEN drive the vehicle.

16. On, or about, January 2, 2019, Detectives assigned to the Saint Louis Metropolitan Police Department's Anti-Crime Task Force observed a dark Chevrolet Impala which appeared to have been involved in the business robberies traveling northbound on Union Boulevard from approximately Maffitt Street. Anti-Crime Detectives attempted to conduct a vehicle stop on the vehicle for their belief the vehicle was involved in a robbery and for observed traffic violations. Upon Detectives' attempt to stop the vehicle, by activating emergency lights and siren, the vehicle fled at a high rate of speed endangering the general public's safety.

17. Eventually, the driver of the Chevrolet Impala, CURTIS ALLEN, brought the vehicle to a stop, exited the driver's seat of the vehicle and fled on foot. ALLEN was taken into custody and charged with several State level crimes based upon this incident which is documented per Saint Louis Metropolitan Police Department complaint number 19-000304.

18. While conducting booking procedures for CURTIS ALLEN, Detectives placed ALLEN'S cellular phone in his prisoner's property bag. This property bag was ultimately conveyed to the property room of the Saint Louis City Justice Center, 200 South Tucker Boulevard. On, or about, April 1, 2019, Investigators obtained a State level search warrant, which was signed by the Honorable Judge Madeline Connolly, ordering the seizure of this cellular phone. The search warrant was executed on this date and Investigators took possession of ALLEN'S cellular phone identified as a:

LG cellular telephone, IMEI: 357093097018786, Serial Number: 808CQRN701878, telephone number 314-446-9922.

19. Later, on, or about April 1, 2019, investigators obtained a State level search warrant, which was signed by the Honorable Judge Elizabeth Hogan, ordering an examination of the seized phone belonging to CURTIS ALLEN. After obtaining the search warrant, Investigators delivered the cellular phone to the Saint Louis Metropolitan Police Department's Cyber Crimes Division.

20. On, or about, April 2, 2019, investigators identified a cellular telephone utilized by MCGEE (314-494-9061) through review of recorded jail calls and toll record analysis. Investigators compared MCGEE's cellular telephone number to ALLEN's call log history which had been obtained from his (ALLEN's) cellular telephone examination. The comparison revealed communication between ALLEN and MCGEE at approximately the same time MCGEE is believed to have left the Smoothie King on November 23, 2018, and the unknown driver of the Chevrolet Impala appeared to answer a telephone call as depicted on surveillance video.

21. Investigators later reviewed the information obtained from the examination of ALLEN'S cellular phone which was seized from his prisoner's property bag. A review revealed the email address INDIAA764@GMAIL.COM is listed as a user account on this cellular phone. Additionally, email activity with this email address was observed on the examination.

22. Investigators later reviewed the information obtained from the examination of ALLEN'S cellular phone which was seized from his prisoner's property bag. A review revealed the email address A1NEYOLA.CA@GMAIL.COM is listed as a user account on this cellular phone. Additionally, email activity with this email address was observed on the examination.

23. In general, an e-mail that is sent to a GOOGLE, LLC subscriber is stored in the subscriber's "mail box" on GOOGLE, LLC servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on GOOGLE, LLC servers

indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on GOOGLE, LLC's servers for a certain period of time.

24. On or about April 10, 2019, JUSTIN MCGEE was arrested pursuant to an authorized arrest warrant issued out of the Eastern District of Missouri on February 15, 2019, Case No. 4:19 MJ 105 DDN, for violation of Title 18, United States Code, Section 1951, Interfering With Commerce With Threats of Violence. During a Mirandized interview, MCGEE confessed to committing thirteen robberies in the St. Louis area between September 2018 and April 2019, to include the aforementioned October 17, 2018, Gamestop robbery; October 12, 2018 T-Mobile robbery; February 4, 2019, Boost Mobile robbery; and November 23, 2018 Smoothie King robbery.

25. During the interview, MCGEE was shown a still photograph from surveillance footage of the aforementioned November 23, 2018, robbery at the Smoothie King. MCGEE acknowledged that the Suspect depicted in the still photograph was him (MCGEE) and MCGEE admitted to committing the robbery, claiming he needed money for gas. MCGEE stated he fled the scene of the robbery in a dark colored Chevrolet Impala driven by one of two unidentified associates "Rick" and "T-Rock", explaining the two were switching driving roles the night of the incident.

26. MCGEE was questioned about the aforementioned December 25, 2018, robbery at the Family Dollar. MCGEE denied committing the robbery, claiming he was at his father's residence at the time. MCGEE said Rick and T-Rock committed the robbery. Following the robbery, Rick and T-Rock came to the residence of MCGEE's father in a dark colored Chevrolet

Impala, where MCGEE helped Rick and T-Rock dispose of a GPS tracking device which had been taken in the robbery.

27. MCGEE was shown still photographs of a dark colored Chevrolet Impala, obtained from surveillance footage of the November 23, 2018 and December 25, 2018 robberies. MCGEE positively identified the vehicle as the getaway vehicle used in multiple robberies MCGEE had committed.

28. MCGEE was shown a photograph of CURTIS ALLEN. MCGEE recognized ALLEN as a friend of Rick, but said he did not know ALLEN well. MCGEE said he did not know that ALLEN owned a dark colored Chevrolet Impala. MCGEE denied that ALLEN drove him to and/or from any robberies.

29. MCGEE acknowledged that he had utilized cellular number 314-494-9061 until approximately one or two months prior to his April 2019 arrest.

30. CURTIS ALLEN was interviewed by investigators on May 7, 2019. During the Mirandized interview, ALLEN acknowledged that he had been the user of cellular number 314-446-9922 from approximately July 2018 until his arrest on or about January 2, 2019. ALLEN stated his Gmail account was A1NEYOLACA@GMAIL.COM, omitting the period from the previously identified Gmail account of A1NEYOLA.CA@GMAIL.COM.

31. ALLEN was shown a photograph of JUSTIN MCGEE, and identified him as JUSTIN, alias name "P-Dog", or "PD". ALLEN has known MCGEE since approximately 2012 or 2013. ALLEN has been a heroin user "off and on" over the years. ALLEN purchased heroin from MCGEE, and the two "got high" together on multiple occasions. In or around the summer of 2018, ALLEN heard that MCGEE was involved in armed business robberies. ALLEN knew

MC GEE to always have a gun on him, stating MCGEE had access to various firearms to include “ARs” and several different handguns.

32. ALLEN was shown a series of text messages communicated between ALLEN’s cellular number, 314-446-9922 and MCGEE’s number 314-494-9061. ALLEN acknowledged that he participated in these conversations with MCGEE, who was utilizing 314-494-9061 at the time.

33. ALLEN acknowledged that he drives a Chevrolet Impala, dark in color, which he purchased in or around 2016. ALLEN said the vehicle is registered in the name of his child’s mother, India Finger. ALLEN was shown still photographs of a dark colored Chevrolet Impala, obtained from surveillance footage of the November 23, 2018 and December 25, 2018 robberies. ALLEN stated the vehicle depicted appeared to be his vehicle; however, ALLEN denied driving MCGEE to or from the robberies, claiming that he loaned his vehicle to MCGEE on those dates.

34. Thus, I believe there is probable cause to believe that information contained in the **Subject Account** will assist in determining ALLEN’s location at and near the time of the November 23, 2018, robbery at the Smoothie King, and the December 25, 2018, robbery at the Family Dollar.

BACKGROUND CONCERNING GOOGLE

35. In my training and experience, and based upon discussions I have had with others familiar with Google, I am informed of the following:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using the Google’s services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity

Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Android ID, Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user’s computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google’s websites). Google also retains information regarding accounts registered from the same IP address.

vii. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

viii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

36. In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

a. *Google Drive content.* Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through a service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud,” that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

c. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

f. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Google Profile.* Google allows individuals to create a Google profile with certain identifying information, including pictures.

i. *Google Plus.* Google hosts an Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply “friends”) into Circles. In addition, Google has a service called PlusOne, in which Google recommends links and posts that may be of interest to the account, based in part on accounts in the user’s Circle having previously clicked “+1” next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user’s Circle.

j. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at <http://www.google.com> (and variations thereof, including <http://www.google.ru>), and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

k. *Advertising Data.* Google also stores advertising data, including information regarding unique advertising IDs associated with the customer, devices used to access the account, application IDs, advertising cookies, Unique Device Identifiers (UDIDs), payment information, ads clicked, and ads created.

l. *YouTube Data.* Google owns the video-streaming service YouTube and maintains records relating to YouTube accesses and data posted by the user.

37. Therefore, the computers of Google and are likely to contain stored electronic communications (including retrieved and unretrieved email) for Google subscribers and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training

and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

38. As explained above, Google subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

39. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

40. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. As explained herein, information stored in connection with a Google account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to

commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

42. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

43. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

44. Based on the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Accounts will contain

evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Attachment A to the proposed warrant.

In particular, I believe the Subject Accounts are likely to contain the following information:

- a) Evidence of the conspiracy to commit the above described armed robbery(s);
- b) Evidence indicating how, when, and where the account was accessed or used, to determine the chronological and geographical context of the account access, use, and events relating to the crime under investigation and to the account owner;
- c) Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and
- d) The identity of the person(s) who created the account and who communicated with the account about the matters relating to the criminal offenses above, including records that help reveal the whereabouts of such persons.

REQUEST FOR NON-DISCLOSURE AND SEALING ORDER

45. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that the target of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

46. Accordingly, there is reason to believe that, were the Providers to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to Title 18, U.S.C. Section 2705(b), I therefore respectfully request that the

Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon the application to the Court, if necessary.

47. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as needed be to personnel assisting in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.


[THE REMAINDER OF THIS PAGE LEFT INTENTIONALLY BLANK]

CONCLUSION

48. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, Title 18, U.S.C. Section 2703(b)(1)(a)(for content) and Section 2703(c)(1)(a)(for records and other information), and the relevant provisions of Federal Rule of Criminal Procedures 41. I submit that there is probable cause to believe that the items identified in Attachment A have been used in the commission of a crime and constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, § 1951 and 924(c)(1) will be found at the premises to be searched as provided in Attachment A.

49. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on GOOGLE, LLC who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



CHRISTOPHER FABER
Special Agent
FBI

Subscribed and sworn to before me on May 14, 2019



SHIRLEY P. MENSAH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property To Be Searched and Items To Be Seized

I. Subject Account and Execution of Warrant

This warrant is directed to Google, Inc, (the "Provider"), headquartered at 1600 Amphitheater Parkway, Mountain View, California 94043, and applies to all subscriber information and location history information within the providers' possession, custody, or control associated with the email accounts INDIAA764@GMAIL.COM, and A1NEYOLA.CA@GMAIL.COM (the "Subject Accounts").

A law enforcement officer will serve the warrant by transmitting it via email or other appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer and electronic copy of the information specified in Section II below. Upon reception of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following associate with the Subject Account for the time period of November 23, 2018 through November 24, 2018 and December 25, 2018 through December 26, 2018, Central Standard Time (CST):

a. All records or other information regarding the identification of the account subscriber and/or user(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and duration, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with

session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account numbers);

- b. All device information associated with the account;
- c. All location history associated with the account, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from
- d. All search and browsing history associated with the account;
- e. The types of services utilized;

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Sections 1951 and 924(c)(1), among other statutes, including the following:

- a. Evidence of the conspiracy to commit the above described armed robbery, and the subsequent efforts to conceal the monetary proceeds;
- b. Evidence indicating how, when, and where the account was accessed or used, to determine the chronological and geographical context of the account access, use, and events relating to the crime under investigation and to the account owner;

c. Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and

d. The identity of the person(s) who created the account and who communicated with the account about the matters relating to the criminal offenses above, including records that help reveal the whereabouts of such persons.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by GOOGLE, LLC, and my official title is _____. I am a custodian of records for GOOGLE, LLC. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of GOOGLE, LLC, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of GOOGLE, LLC; and
- c. such records were made by GOOGLE, LLC as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature